Доклады Академии Наук СССР
1953. Том XCI, № 4

МАТЕМАТИКА

В. А. УСПЕНСКИЙ

ТЕОРЕМА ГЁДЕЛЯ И ТЕОРИЯ АЛГОРИТМОВ

(Представлено академиком А. Н. Колмогоровым 8 VI 1953)

1. Предварительные замечания. В работе [3] Гёдель показал, что попытка аксиоматического построения арифметики неизбежно приводит к дедуктивно-неполному исчислению, т. е. к исчислению, в котором существует формула, интерпретируемая как содержательно-истинное высказывание о натуральных числах и вместе с тем недоказуемая в этом исчислении. Более того в [3] был указан эффективный способ построения такой формулы. Настоящая заметка содержит результаты предпринятого по инициативе А. Н. Колмогорова выяснения общих причин такого положения вещей. При этом обнаруживается роль теории алгоритмов в вопросах дедуктивной полноты.

Мы скажем, что множество натуральных чисел R порождается функцией φ, если R есть множество значений φ. Каждой системе равенств, задающей частично-рекурсивную функцию φ, можно отнести некоторое натуральное число, по которому система равенств однозначно восстанавливается; это число называется номером функции φ [5]. Номером рекурсивно-перечислимого множества R мы назовем любое число, являющееся одним из номеров одной из частично-рекурсивных функций, порождающих R.

2. Эффективная неотделимость. Говорят, что множества E_1 и E_2 отделяются множествами H_1 и H_2, если $E_1 \subseteq H_1$, $E_2 \subseteq H_2$, $H_1 \cap H_2 = \Lambda$. Множества E_1 и E_2 называются рекурсивно-неотделимыми [2], а короче — неотделимыми, если они не отделяются никакими рекурсивными множествами. Можно построить два непересекающихся рекурсивно-перечислимых множества, являющихся неотделимыми (впервые такие множества построены П. С. Новиковым; дальнейшие примеры принадлежат Б. А. Трахтенброту [2]).

Введем понятие эффективной неотделимости. Множества E_1 и E_2 назовем эффективно-неотделимыми, коль скоро существует такая частично-рекурсивная функция $\nu(x, y)$, что если n_1 и n_2 суть номера рекурсивно-перечислимых множеств H_1 и H_2, отделяющих E_1 и E_2, то $\nu(n_1, n_2)$ существует, но не принадлежит $H_1 \cup H_2$.

Теорема 1. *Существуют два эффективно-неотделимых непересекающихся рекурсивно-перечислимых множества.*

Более того, эффективно-неотделимыми являются все известные до сего времени неотделимые множества.

3. Дедуктивные исчисления. Для любого конечного множества $\mathfrak{Z}$ «знаков» будем обозначать через $\mathfrak{S}(\mathfrak{Z})$ множество всевозможных конечных строчек, составленных из этих знаков («слов в алфавите $\mathfrak{Z}$» по А. А. Маркову [1]). Знаки из $\mathfrak{Z}$ занумеруем числами $1, 2, \ldots, n$, где n — число знаков в $\mathfrak{Z}$; каждой строчке $A = \alpha_1\alpha_2\ldots\alpha_j$,

где α_μ суть знаки из $\mathfrak{Z}$, отнесем в качестве номера число $N(A) = 2^{b(\alpha_1)} \cdot 3^{b(\alpha_2)} \cdot \ldots \cdot p_j^{b(\alpha_j)}$, где p_j есть j-е простое число, а $b(\alpha)$ — номер знака α.

Дедуктивное исчисление П есть совокупность следующих образований: 1) конечного множества $\mathfrak{Z}$ элементарных знаков (строчки из $\mathfrak{S}(\mathfrak{Z})$ называются «формулами» исчисления П); 2) конечного множества $A_1, \ldots, A_p$ формул из $\mathfrak{S}(\mathfrak{Z})$, называемых «аксиомами»; 3) конечного множества $\Gamma_1, \ldots, \Gamma_q$ алгоритмов, называемых «правилами вывода». При этом алгоритм Γ_i $(i = 1, 2, \ldots, q)$ способен «перерабатывать» лишь строчки вида $X_1, X_2, \ldots, X_{k_i}, Y_1, Y_2, \ldots, Y_{l_i}$, где k_i и l_i — фиксированные неотрицательные числа, X_μ и Y_ν — формулы из $\mathfrak{S}(\mathfrak{Z})$, а запятая «,» — знак, не входящий в $\mathfrak{Z}$. Для любой строчки описанного сейчас вида алгоритм Γ_i или дает формулу из $\mathfrak{S}(\mathfrak{Z})$ или ничего не дает. В целях уточнения термина «алгоритм» примем следующее основное допущение: если $Z = \Gamma_i(X_1, \ldots, X_{k_i}, Y_1, \ldots, Y_{l_i})$, то $N(Z) = \varphi_i(N(X_1), \ldots \ldots, N(X_{k_i}), N(Y_1), \ldots, N(Y_{l_i}))$, где φ_i — частично-рекурсивная функция.

В $\mathfrak{S}(\mathfrak{Z})$ образуется подмножество выводимых формул по следующему закону: все аксиомы выводимы; далее, если $X_1, \ldots, X_{k_i}$ выводимы и $Z = \Gamma_i(X_1, \ldots, X_{k_i}, Y_1, \ldots, Y_{l_i})$, то и Z выводима. Понятие дедуктивного исчисления можно несколько сузить, потребовав, чтобы для каждого правила вывода Γ_i существовал алгоритм Δ_i, позволяющий для всякой строчки $X_1, \ldots, X_{k_i}, Y_1, \ldots, Y_{l_i}$ определять, принадлежит она области применимости Γ_i или нет. Для дальнейшего безразлично, как понимать термин «дедуктивное исчисление» — в широком смысле или в узком: все утверждения, которые будут высказаны, остаются справедливыми при обоих пониманиях.

Ниже мы будем рассматривать лишь исчисления «с отрицанием», т. е. удовлетворяющие условию: 4) в $\mathfrak{Z}$ выделен некоторый определенный знак, для которого примем стандартное обозначение $\neg$. Если A — формула, то формулу $\neg A$ назовем отрицанием A; формулу $\underbrace{\neg\neg\ldots\neg}_{n \text{ раз}} A$ назовем n-кратным отрицанием A.

Рассмотрим произвольное подмножество $\mathfrak{B} \subseteq \mathfrak{S}(\mathfrak{Z})$, обладающее следующими свойствами: а) существует алгоритм, позволяющий для всякой формулы $A \in \mathfrak{S}(\mathfrak{Z})$ определить, принадлежит A к $\mathfrak{B}$ или нет; б) если $A \in \mathfrak{B}$, то и $\neg A \in \mathfrak{B}$. Можно показать, что эти свойства множества $\mathfrak{B}$ не зависят от того, в каком объемлющем множестве $\mathfrak{S}(\mathfrak{Z})$ мы его рассматриваем. Исчисление П высекает в $\mathfrak{B}$ подмножество $\mathfrak{K}_{\mathfrak{B}}(\text{П})$ выводимых формул и подмножество $\mathfrak{L}_{\mathfrak{B}}(\text{П})$ формул, отрицания которых выводимы. В применении к $\mathfrak{B}$ исчисление П называется непротиворечивым, если $\mathfrak{K}_{\mathfrak{B}}(\text{П}) \cap \mathfrak{L}_{\mathfrak{B}}(\text{П}) = \Lambda$, и полным, если $\mathfrak{K}_{\mathfrak{B}}(\text{П}) \cup \mathfrak{L}_{\mathfrak{B}}(\text{П}) = \mathfrak{B}$. Исчисление П′ назовем усилением исчисления П в применении к $\mathfrak{B}$, если $\mathfrak{K}_{\mathfrak{B}}(\text{П}') \supseteq \mathfrak{K}_{\mathfrak{B}}(\text{П})$. Исчисление П назовем непополнимым в применении к $\mathfrak{B}$, если оно не допускает полного и непротиворечивого усиления. Множества номеров, соответствующие множествам $\mathfrak{K}_{\mathfrak{B}}(\text{П})$ и $\mathfrak{L}_{\mathfrak{B}}(\text{П})$, обозначим через $K_{\mathfrak{B}}(\text{П})$ и $L_{\mathfrak{B}}(\text{П})$; легко показать, что оба эти множества рекурсивно-перечислимы. Исчисление П назовем эффективно-непополнимым в применении к $\mathfrak{B}$, коль скоро существует такая частично-рекурсивная функция $\gamma(x)$, что если n есть номер рекурсивно-перечислимого множества $K_{\mathfrak{B}}(\text{П}')$, где П′ — непротиворечивое усиление исчисления П, то $\gamma(n)$ есть номер формулы из $\mathfrak{B}$, неразрешимой в П′. При этом формула называется неразрешимой в исчислении, если ни она, ни ее отрицание не выводимы в этом исчислении. В дальнейшем множество $\mathfrak{B}$ будет всегда фиксированным,

поэтому слова «в применении к $\mathfrak{B}$», равно как и индекс $\mathfrak{B}$ будут для краткости в большинстве случаев опускаться.

4. Регулярные исчисления. Дедуктивное исчисление Π назовем D_1-исчислением в применении к $\mathfrak{B}$, если для всякой формулы $A \in \mathfrak{B}$ из выводимости A следует выводимость $\neg\neg A$. Дедуктивное исчисление Π назовем регулярным в применении к $\mathfrak{B}$, если оно есть D_1-исчисление и для всякой формулы $A \in \mathfrak{B}$ из выводимости $\neg\neg\neg A$ следует выводимость $\neg A$.

Теорема 2. *Необходимым и достаточным условием непополнимости регулярного исчисления* Π *является неотделимость множеств* $K(\Pi)$ *и* $L(\Pi)$.

Следуя Тарскому ([6]) назовем исчисление Π разрешимым в применении к $\mathfrak{B}$, если $K(\Pi)$ есть рекурсивное множество, и существенно неразрешимым, если Π непротиворечиво и не допускает непротиворечивого разрешимого усиления.

Теорема 3. *Регулярное исчисление тогда и только тогда существенно неразрешимо, когда оно непротиворечиво и непополнимо* (ср. ([6])).

Теорема 4. *Эффективная неотделимость* $K(\Pi)$ *и* $L(\Pi)$ *необходима и достаточна для эффективной непополнимости регулярного исчисления* Π.

Отнесем к множеству $\mathfrak{X}(\mathfrak{B})$ всякую формулу $A \in \mathfrak{B}$, для которой не существует формулы $B \in \mathfrak{B}$ такой, что $\neg B = A$.

Теорема 5. *Пусть* D_1-*исчисление* Π *эффективно-непополнимо в применении к* $\mathfrak{B}$. *Тогда существует такая частично-рекурсивная функция* $\tilde{\gamma}(x)$, *что если* n *есть номер рекурсивно-перечислимого множества* $K_{\mathfrak{B}}(\Pi')$, *где* Π' *непротиворечивое усиление* Π, *то* $\tilde{\gamma}(n)$ *есть номер формулы из* $\mathfrak{X}(\mathfrak{B})$, *неразрешимой в* Π'.

5. Применение к теореме Гёделя. Пусть для каждого натурального m определена формула $F(m) \in \mathfrak{S}(\mathfrak{Z})$, причем выполняются следующие условия: а) существует обще-рекурсивная функция $f(x)$ такая, что $f(m)$ есть номер формулы $F(m)$; б) множество номеров формул $F(m)$ рекурсивно. Пусть, далее, E_1 и E_2 — эффективно-неотделимые множества. Образуем множество $\mathfrak{B}$, состоящее из всех формул вида $\neg\neg\ldots\neg F(m)$. Можно построить дедуктивное исчисление Π_0 такое, что $\mathfrak{K}(\Pi_0)$ состоит из четнократных отрицаний формул $F(m)$ при $m \in E_1$ и нечетнократных отрицаний $F(m)$ при $m \in E_2$. Легко показать, что $K(\Pi_0)$ и $L(\Pi_0)$ эффективно-неотделимы. Применяя последовательно теоремы 4 и 5, получаем, что для всякого непротиворечивого исчисления Π', являющегося усилением исчисления Π_0, алгоритмически строится формула $F(m)$, неразрешимая в Π'; более точно, существует такая частично-рекурсивная функция $\zeta(x)$, что если n — номер $K(\Pi')$, где Π' — непротиворечивое усиление Π_0, то $F(\zeta(n))$ неразрешима в Π'.

Отсюда легко следует теорема Гёделя. В качестве E_1 и E_2 возьмем какие-нибудь непересекающиеся эффективно-неотделимые рекурсивно-перечислимые множества (см. теорему 1). Известно ([4]), что всякое рекурсивно-перечислимое множество может быть порождено примитивно-рекурсивной функцией. Пусть $\theta_1(x)$ и $\theta_2(x)$ — примитивно-рекурсивные функции, порождающие, соответственно, E_1 и E_2. Положим

$$F(m) = (Ex)\,(\theta_1(x) = m \,\&\, (y)\,(y \leqslant x \rightarrow \neg\,(\theta_2(y) = m))).$$

Формула $F(m)$ содержательно эквивалентна утверждению $m \in E_1$. Построим, как указано, множество формул $\mathfrak{B}$ и исчисление Π_0. Обычно дедуктивные исчисления, описывающие арифметику, являются усилениями Π_0, поэтому для каждого из них алгоритмически указывается

неразрешимая формула $F(m)$. Нам остается заметить, что для всякого m из неразрешимости $F(m)$ вытекает, что $\neg F(m)$ истинна, но невыводима.

6. Нерегулярные исчисления.

Теорема 6. *Неотделимость* $K(\Pi)$ *и* $L(\Pi)$ *достаточна для непополнимости произвольного исчисления* Π.

Теорема 7. *Если* $\mathfrak{B}$ *таково, что* $\mathfrak{X}(\mathfrak{B})$ *бесконечно, то существует непротиворечивое исчисление, являющееся непополнимым разрешимым* D_1*-исчислением в применении к* $\mathfrak{B}$.

Из теоремы 7 следует, что теоремы 2 и 3 перестают быть верными при замене слов «регулярное исчисление» словами «D_1-исчисление».

Теорема 8. *Эффективная неотделимость* $K(\Pi)$ *и* $L(\Pi)$ *достаточна для эффективной непополнимости произвольного исчисления* Π.

Отнесем к множеству $\mathfrak{K}^+(\Pi)$ всякую формулу A, обладающую следующими свойствами: а) $A \in \mathfrak{X}(\mathfrak{B})$; б) существует такое четное число s, что s-кратное отрицание A принадлежит $\mathfrak{K}(\Pi)$. Аналогично строится множество $\mathfrak{L}^+(\Pi)$. Соответствующие множества номеров обозначим $K^+(\Pi)$ и $L^+(\Pi)$. Исчисление Π назовем согласованным в применении к $\mathfrak{B}$, если $\mathfrak{K}^+(\Pi) \cap \mathfrak{L}^+(\Pi) = \Lambda$. Из согласованности исчисления следует его непротиворечивость; в регулярном случае эти понятия совпадают.

Теорема 9. *Всякое несогласованное исчисление непополнимо.*

Теорема 10. *Необходимым и достаточным условием непополнимости согласованного исчисления* Π *является неотделимость множеств* $K^+(\Pi)$ *и* $L^+(\Pi)$.

Назовем исчисление Π слабо эффективно-непополнимым в применении к $\mathfrak{B}$, коль скоро существует такая частично-рекурсивная функция $\delta(x)$, что если n — номер множества $K(\Pi')$, где Π' — согласованное усиление исчисления Π, то $\delta(n)$ есть номер формулы из $\mathfrak{B}$, неразрешимой в Π'.

Теорема 11. *Необходимым и достаточным условием слабой эффективной непополнимости согласованного исчисления* Π *является эффективная неотделимость множеств* $K^+(\Pi)$ *и* $L^+(\Pi)$.

7. Проблемы. В заключение сформулируем несколько нерешенных, связанных с изложенным выше, проблем:

I. Существуют ли неотделимые множества, не являющиеся эффективно-неотделимыми?

II. Существует ли непополнимое исчисление, не являющееся эффективно-непополнимым?

III. Является ли эффективная неотделимость $K(\Pi)$ и $L(\Pi)$ необходимой для эффективной непополнимости нерегулярных исчислений?

IV. Существует ли слабо эффективно-непополнимое исчисление, не являющееся эффективно-непополнимым?

V. Существует ли непополнимое исчисление, не являющееся слабо эффективно-непополнимым?

Автор благодарен А. Н. Колмогорову за ряд советов. В частности, А. Н. Колмогорову принадлежит определение «исчисления» и указание на достаточность условия теоремы 2.

Поступило
22 V 1953

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. А. Марков, Тр. Матем. ин-та им. Стеклова АН СССР, 38, 176 (1951). [2] Б. А. Трахтенброт, ДАН, 88, 953 (1953). [3] K. Gödel, Monatsh. f. Math. u. Phys., 38, 173 (1931). [4] J. B. Rosser, J. Symb. Logic, 1, 87 (1936). [5] S. C. Kleene, Trans. Am. Math. Soc., 53, 41 (1943). [6] A. Tarski, J. Symb. Logic, 14, 75 (1949).